(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 859 340 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.08.1998 Bulletin 1998/34

(51) Int. Cl.[6]: **G07B 17/00**

(21) Application number: **97120460.7**

(22) Date of filing: **21.11.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.11.1996 US 754578**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

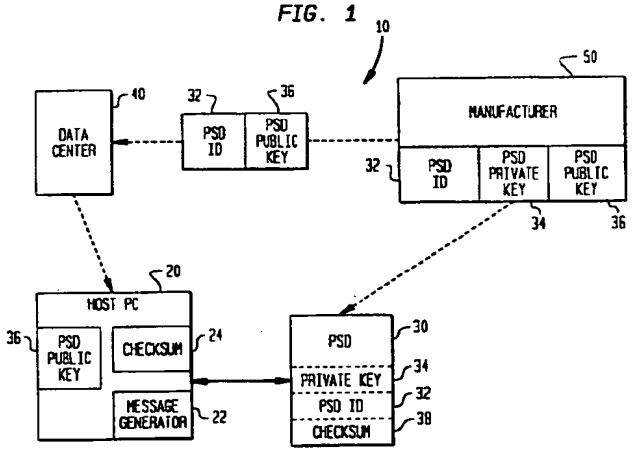
(72) Inventors:
- **Ryan, Frederick W., Jr.**
  Oxford, Connecticut 06478 (US)
- **Cordery, Robert A.**
  Danbury, Conn. 06811 (US)

(74) Representative:
Avery, Stephen John et al
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Method for verifying the expected postage security device and its status

(57) A secure and reliable method for verifying in the host system that the expected PSD is coupled to the host system includes generating a random number in the host system and encrypting the random number with a PSD state identification number. The encrypted random number is then sent to the PSD. The PSD decrypts the encrypted random number received using the PSD state identification number and sends the decrypted random number to the host system. The host system compares the decrypted random number received from the PSD to the random number generated in the host system. If they are the same, the host system has verified the expected PSD and has also verified that the PSD has not completed any transactions apart from the host system. A method for verifying that the expected host is coupled to the PSD mirrors the method for verifying the expected PSD.

FIG. 1



EP 0 859 340 A2

BNSDOCID: <EP 0859340A2_I_>

Description

The present invention relates generally to a system and method for postage metering security and, more particularly, to systems and methods for verifying authorized postage security devices.

The Information-Based Indicia Program (IBIP) is a distributed trusted system proposed by the United States Postal Service (USPS). The IBIP is expected to support new methods of applying postage in addition to, and eventually in lieu of, the current approach, which typically relies on a postage meter to mechanically print indicia on mailpieces. The IBIP requires printing large, high density, two dimensional (2-D) bar codes on mailpieces. The Postal Service expects the IBIP to provide cost-effective assurance of postage payment for each mailpiece processed.

The USPS has published draft specifications for the IBIP. The INFORMATION BASED INDICIA PROGRAM (IBIP) INDICIUM SPECIFICATION, dated June 13, 1996 defines the proposed requirements for a new indicium that will be applied to mail being processed using the IBIP. The INFORMATION BASED INDICIA PROGRAM POSTAL SECURITY DEVICE SPECIFICATION, dated June 13, 1996, defines the proposed requirements for a Postal Security Device (PSD) that will provide security services to support the creation of a new "information based" postage postmark or indicium that will be applied to mail being processed using the IBIP. The INFORMATION BASED INDICIA PROGRAM HOST SYSTEM SPECIFICATION, dated October 9, 1996, defines the proposed requirements for a host system element of the IBIP. The specifications are collectively referred to herein as the "IBIP Specifications". The IBIP includes interfacing user (customer), postal and vendor infrastructures which are the system elements of the program.

The user infrastructure, which resides at the user's site, comprises a postage security device (PSD) coupled to a host system. The PSD is a secure processor-based accounting device that dispenses and accounts for postal value stored therein. The host system may be a personal computer (PC) or a meter-based host processor. Among the various requirements set forth in the Host System Specification is that the host system verifies that the coupled PSD is "the expected PSD". Conventional postage metering devices and recent digital metering devices, such as PostPerfect and Personal Post Office, both manufactured by the assignee of the present invention, do not include such verification. Thus, a method for achieving such verification is desired.

U.S. Patent No. 5,510,992 discloses a method whereby the host PC verifies that a storage means that is coupled to the host PC and has postal value stored therein, is authorized far use with the host PC. The method comprises the steps of storing a unique identifier, such as a serial number, in the storage means when the storage means is filled with postal value, and sending the unique identifier to the host PC when postage value is requested for dispensing. The host PC then verifies that the storage means is authorized for use with the host PC by confirming that the unique identifier retrieved from the storage device is the same as one stored in the host PC. Although such method verifies that the storage means is the expected storage device, the storage means is not a PSD because it is not a processor-based accounting device that dispenses and accounts for postal value stored therein. Furthermore, the verification of the serial number in the host PC is subject to fraud.

It has been found that the present invention provides a more secure and reliable system and method for verifying the expected PSD is coupled to the host PC. It has further been found that the present invention provides a secure and reliable system and method for verifying the expected host PC is coupled to the PSD.

The present invention provides a secure and reliable method for verifying in the host system that the expected PSD is coupled to the host system. In accordance with the present invention, a random number is generated in the host system and encrypted with a PSD state identification number. The encrypted random number is then sent to the PSD. The PSD decrypts the encrypted random number received using the PSD state identification number and sends the decrypted random number to the host system. The host system compares the decrypted random number received from the PSD to the random number generated in the host system. If they are the same, the host system has verified the expected PSD and has also verified that the PSD has not completed any transactions apart from the host system. A method for verifying that the expected host is coupled to the PSD mirrors the method for verifying the expected PSD.

The above and other objects and advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

Fig. 1 is a block diagram of a postage metering system in accordance with the present invention showing a process for storing keys in a host system and a PSD coupled thereto;
Fig. 2 is a flow chart showing an alternate process for storing keys in a host system and a PSD coupled thereto;
Fig. 3 is a flow chart of a preferred method for verifying the expected PSD is coupled to the host system; and
Fig. 4 is a flow chart of showing a method corresponding to that of Fig. 3 for verifying the expected host system.

In describing the present invention, reference is

BNSDOCID: <EP___0859340A2_I_>

made to the drawings, wherein there is seen system and methods for verifying the expected postage security device in a host system and conversely verifying the expected host system. Referring now to Fig. 1, a postage metering system, generally designated 10, includes a Host PC 20 coupled to a PSD 30, a Data Center 40 and a manufacturer 50. The manufacturer 50 initializes PSD 30 with an identification number such as PSD ID 32, and a cryptographic key, such as PSD private key 34. The manufacturer 50 also sends the PSD ID 32 and a cryptographic key corresponding to the key in the PSD 30, such as PSD public key 36, to the Data Center 40. The Data Center 40 then sends the PSD ID 32 and the public key 36, to the Host PC 20. For the purpose of describing the present invention, the PSD private and public keys are stored in PSD 30 and Host PC 20 respectively. It will be understood that a secret key shared by the Host PC and the PSD may be used in place of such key pair.

The Host PC 20 and PSD 30 each include a microprocessor and memory (not shown). The Host PC 20 further includes a message generator 22 for generating a message. The message may be a random number or may include data indicating status of the PSD, for example a checksum 24 of PSD transaction records stored a log files in Host PC 20. For the following description of the present invention checksums will be used. The PSD records stored in Host PC 20 correspond to PSD records stored in PSD 30 for each transaction by PSD 30. For a more detailed description of such storage of PSD records see European Patent Publication Number 0780808, assigned to the assignee of the present invention, and which is incorporated herein by reference.

Referring now to Fig. 2, an alternate method for initialising the PSD with a cryptographic key is shown. At step 100, Host PC 20 generates a secret key or a key pair. The key or key pair is stored in Host PC 20, at step 105. Host PC 20 the sends the secret key or one of the keys of the key pair to PSD 30, at step 110. PSD 30 stores the key received from Host PC 20, at step 115.

Referring now to Fig. 3, a method is shown for verifying in Host PC 20 that the expected PSD is coupled thereto. At step 200, the Host PC generates a random number which is then encrypted, at step 205, with a PSD state identification number or data. In the preferred embodiment of the present invention, the PSD state identification number or data represents a predetermined status of the PSD after the previous transaction between the Host PC and the PSD. For example, the PSD state identification number or data may be a checksum of the PSD transaction logs or the last random number generated for the purpose of verifying the PSD. At step 210, the encrypted random number is sent to the PSD. At step 215, the PSD decrypts the encrypted random number received from the Host PC using the same PSD state identification number or data that was used by the Host PC. At step 220, the PSD sends the decrypted random number, (or a message derived therefrom), to the Host PC.

At step 225, the Host PC verifies that the random number received from the PSD is the same as the random number generated in the Host PC. (or that the message derived therefrom corresponds to the random number). If not the same at step 230, the Host PC flags an error and rejects the PSD from processing any further transactions, at step 235. If the random number received from the PSD is the same as the random number generated in the Host PC, at step 240, the Host PC has verified that the expected PSD is coupled to the Host PC and has not processed any transactions apart from the Host PC. Thus, the Host PC can begin requesting postal value from the PSD.

Referring now to Fig. 4, it may be required that in addition to the Host PC verifying the expected PSD, the PSD verify that the expected Host PC is coupled to the PSD. In the preferred embodiment of the present invention, such verification of the expected Host PC mirrors the process for verifying the expected PSD as set forth above.

At step 300, the PSD generates a random number which is then encrypted, at step 305, with a PSD state identification number or data. At step 310, the encrypted random number is sent to the Host PC. At step 315, the Host PC decrypts the encrypted random number received from the PSD using the same PSD state identification number or data that was used by the PSD. At step 320, the Host PC sends the decrypted random number to the PSD.

At step 325, the PSD verifies that the random number received from the Host PC is the same as the random number generated in the PSD. If not the same at step 330, the PSD flags an error which prevents the PSD from processing any further transactions, at step 335. If the random number received from the Host PC is the same as the random number generated in the PSD, at step 340, the PSD has verified that the expected Host PC is coupled to the PSD and the PSD has not processed any transactions apart from the Host PC.

It has been found that the present invention is suitable for use with any security device that is coupled to a host system in an unsecured manner. For example, the present invention could be used for a certificate metering system such as disclosed in European Patent Publication No. 0762692, filed August 21, 1996, assigned to the assignee of the present invention, and which is incorporated herein by reference.

While the present invention has been disclosed and described with reference to specific embodiments thereof, it will be apparent, as noted above,that variations and modifications may be made therein. It is, thus, intended in the following claims to cover each variation and modification, including a certificate metering system, that falls within the true spirit and scope of the present invention.

BNSDOCID: <EP__0859340A2_I_>

Claims

1. A method for verifying in a host system that a postage security device (PSD) is the expected PSD and that the PSD has not completed transactions with other than the host system, the method comprising the steps of:

   generating a first message in the host system;
   generating in the host system first identification data using first transaction records stored in the host system, said first identification data representing a predetermined status of the PSD after the previous transaction between the host system and the PSD;
   encrypting the first message with the first identification data;
   sending the encrypted first message to the PSD;
   generating in the PSD second identification data using second transaction records stored in the PSD, said second identification data representing the predetermined status of the PSD after the previous transaction between the host system and the PSD;
   decrypting the encrypted first message with the second identification data;
   sending to the host system a second message derived from the decrypted first message; and
   verifying in the host system that the second message corresponds to the first message.

2. The method of claim 1 wherein the first message includes data indicating status of the PSD based on PSD transaction records stored in the host system.

3. The method of claim 1 wherein the second message is the decrypted first message and the step of verifying verifies that the second message is the same as the first message.

4. The method of claim 2 wherein the data indicating status of the PSD is a checksum of PSD transaction records.

5. A method for verifying in a computer system that a microprocessor-based system is the expected microprocessor-based system and that the microprocessor-based system has not completed transactions with other than the computer system, the method comprising the steps of:

   generating a message in the computer system;
   generating in the computer system first identification data using first transaction information stored in the computer system, said first identification data representing a predetermined status of the microprocessor-based system after the previous transaction between the computer system and the microprocessor-based system;
   encrypting the message with the identification data;
   sending the encrypted message to the microprocessor-based system;
   generating in the microprocessor-based system second identification data using second transaction information stored in the microprocessor-based system, said second identification data representing the predetermined status of the microprocessor-based system after the previous transaction between the computer system and the microprocessor-based system;
   decrypting the message with the second identification data;
   sending a message derived from the decrypted message to the computer system; and
   verifying in the computer system that the derived message corresponds to the generated message.

6. The method of claim 1 or 5 wherein the message generated is random data.

7. The method of claim 5 wherein the message generated includes data indicating status of the microprocessor-based system based on microprocessor-based system transaction records stored in the computer system.

8. The method of claim 7 wherein the data indicating status of the microprocessor-based system is a checksum of the microprocessor-based system transaction records.

9. The method of claim 1 or 5 wherein the computer system is a personal computer.

10. The method of claim 1 or 5 wherein the first and second identification data include at least one of a checksum, control sum, ascending register, descending register and random data from the previous transaction.

11. The method of claim 5 wherein the derived message is the decrypted message and the step of verifying verifies that the decrypted message is the same as the generated message.

12. A method for verifying in a host system that a postage security device (PSD) is the expected PSD, that the host system is the expected host system and that the PSD has not completed transactions with other than the host system, the method comprising the steps of:

    generating a first message in the host system;

BNSDOCID: <EP___0859340A2_I_>

generating in the host system first identification data using first transaction records stored in the host system, said first identification data representing a predetermined status of the PSD after the previous transaction between the host system and the PSD;

encrypting the first message with the first identification data;

sending the encrypted first message to the PSD:

generating in the PSD second identification data using second transaction records stored in the PSD, said second identification data representing the predetermined status of the PSD after the previous transaction between the host system and the PSD;

decrypting the encrypted first message with the second identification data;

sending a message derived from the decrypted first message to the host system;

verifying in the host system that the message derived from the decrypted first message corresponds to the generated first message;

generating a second message in the PSD;

encrypting the second message with the second identification data;

sending the encrypted second message to the host system;

decrypting the encrypted second message with the first identification data;

sending a message derived from the decrypted second message to the PSD; and

verifying in the PSD that the message derived from the decrypted second message corresponds to the generated second message

13. The method of claim 12 wherein the message derived from the decrypted first message is the decrypted first message and the message derived from the decrypted second message is the decrypted second message.

BNSDOCID: <EP___0859340A2_I_>

FIG. 1

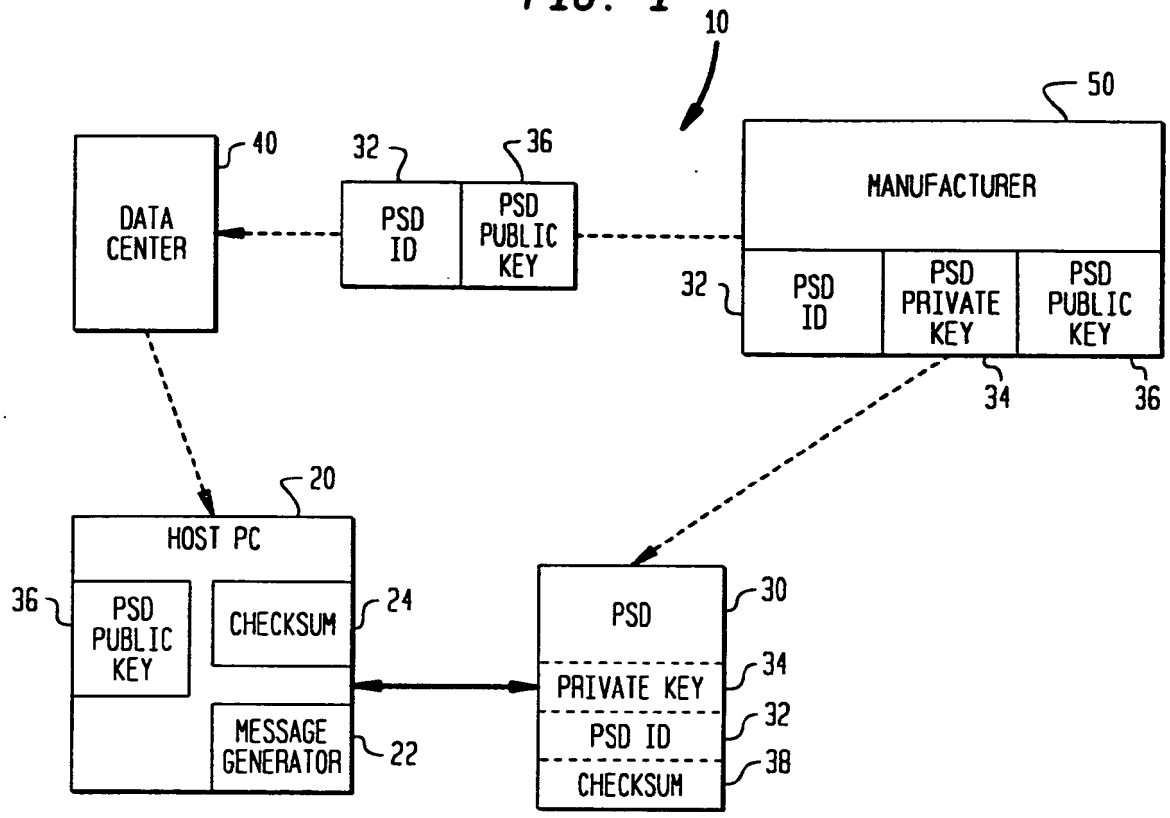
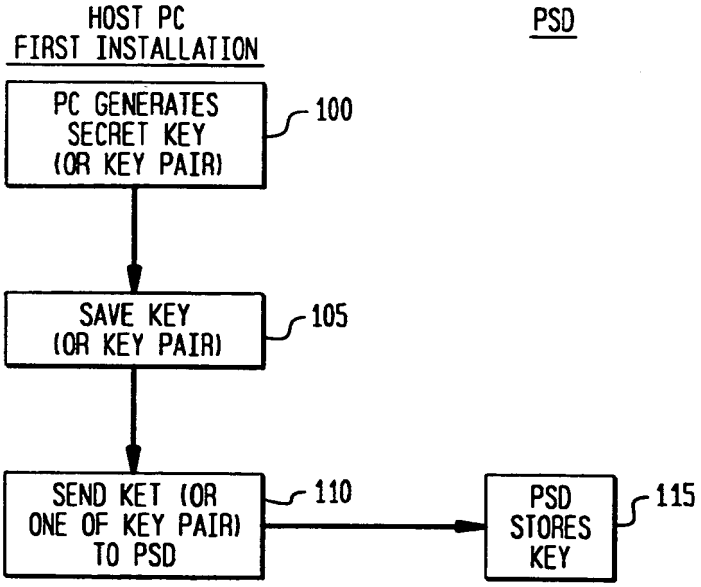
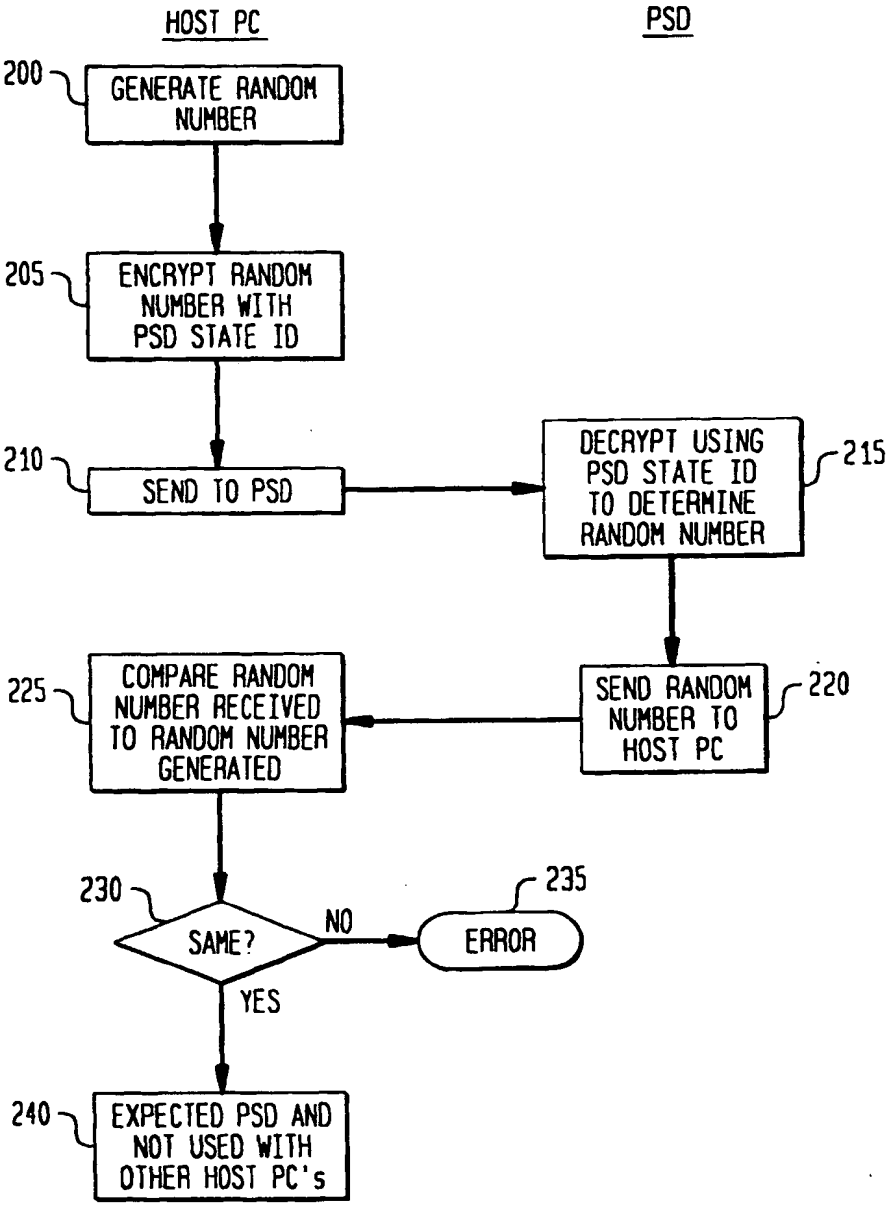


FIG. 2



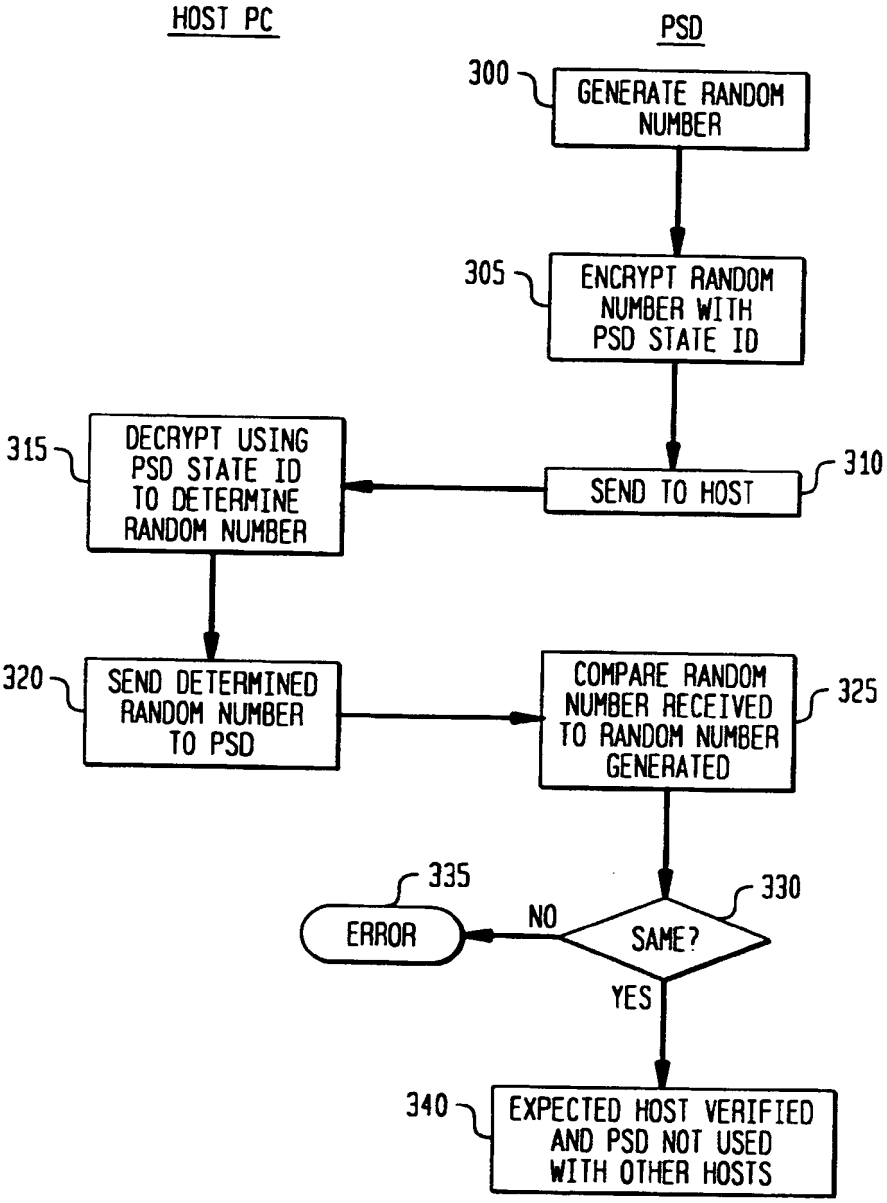
BNSDOCID: <EP___0859340A2_I_>

FIG. 3



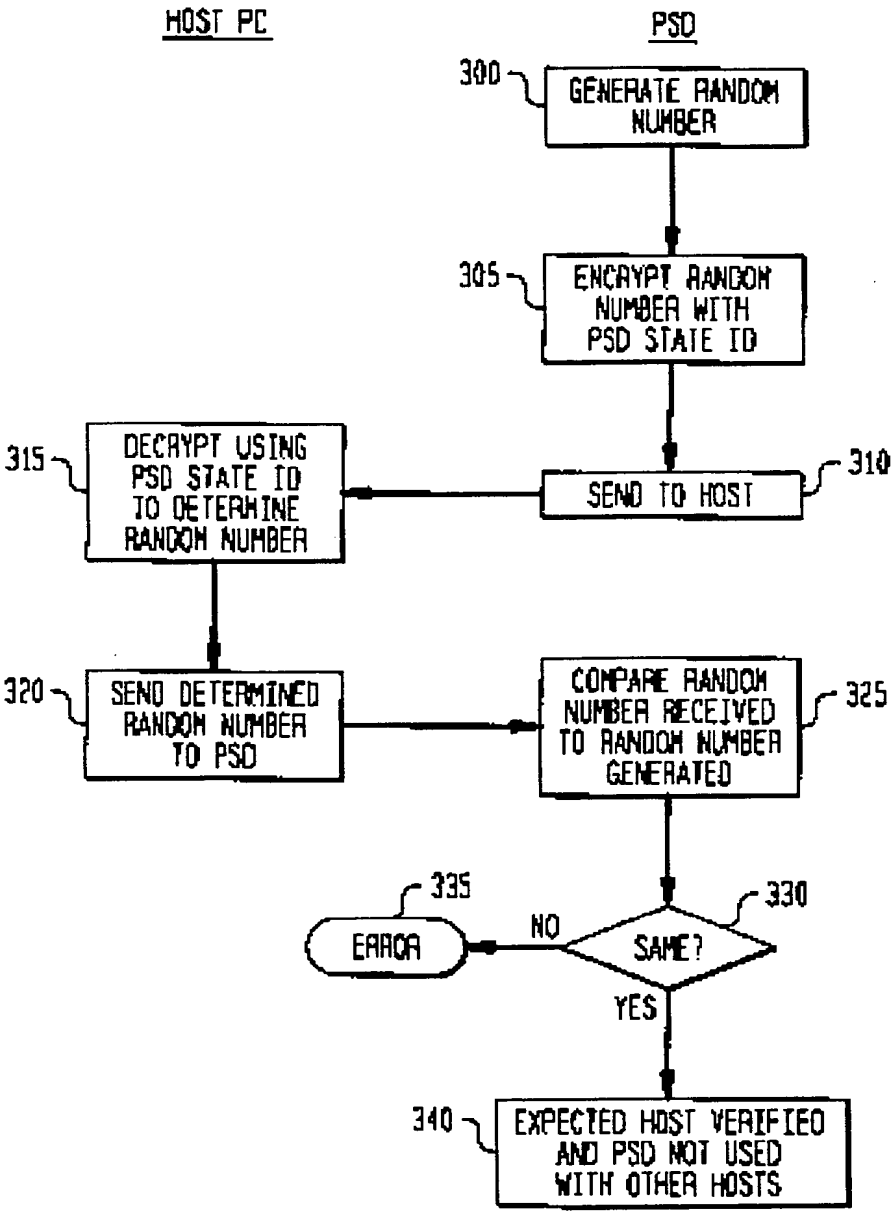
BNSDOCID <EP___0859340A2_I_>

FIG. 4



BNSDOCID: <EP___0859340A2_I_>

FIG. 4



BNSDOCID: <EP___0859340A2T1_>

FIG. 1

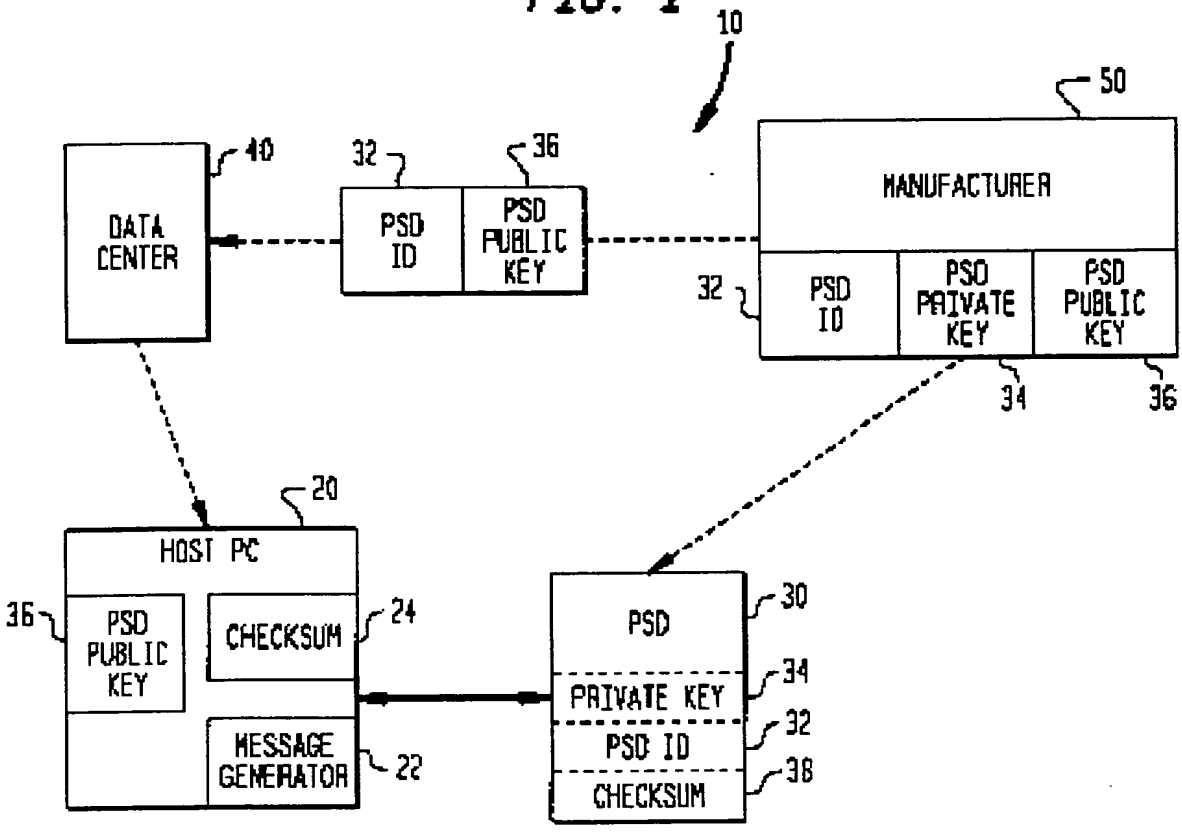
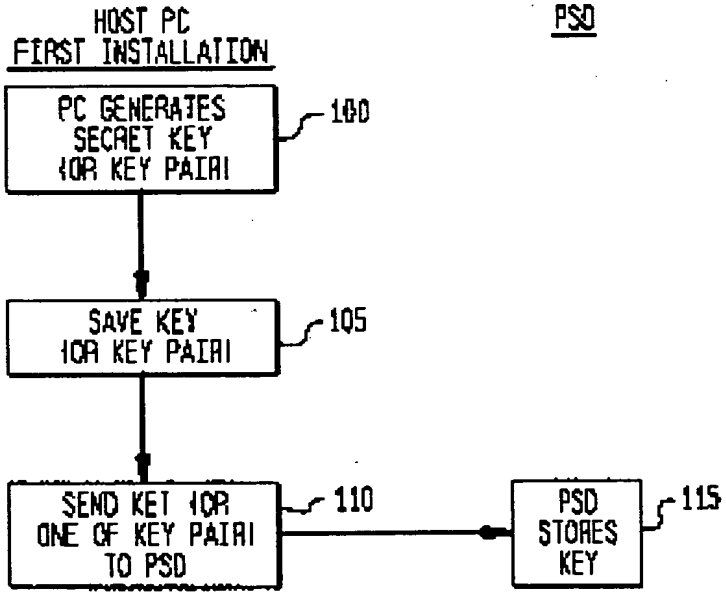
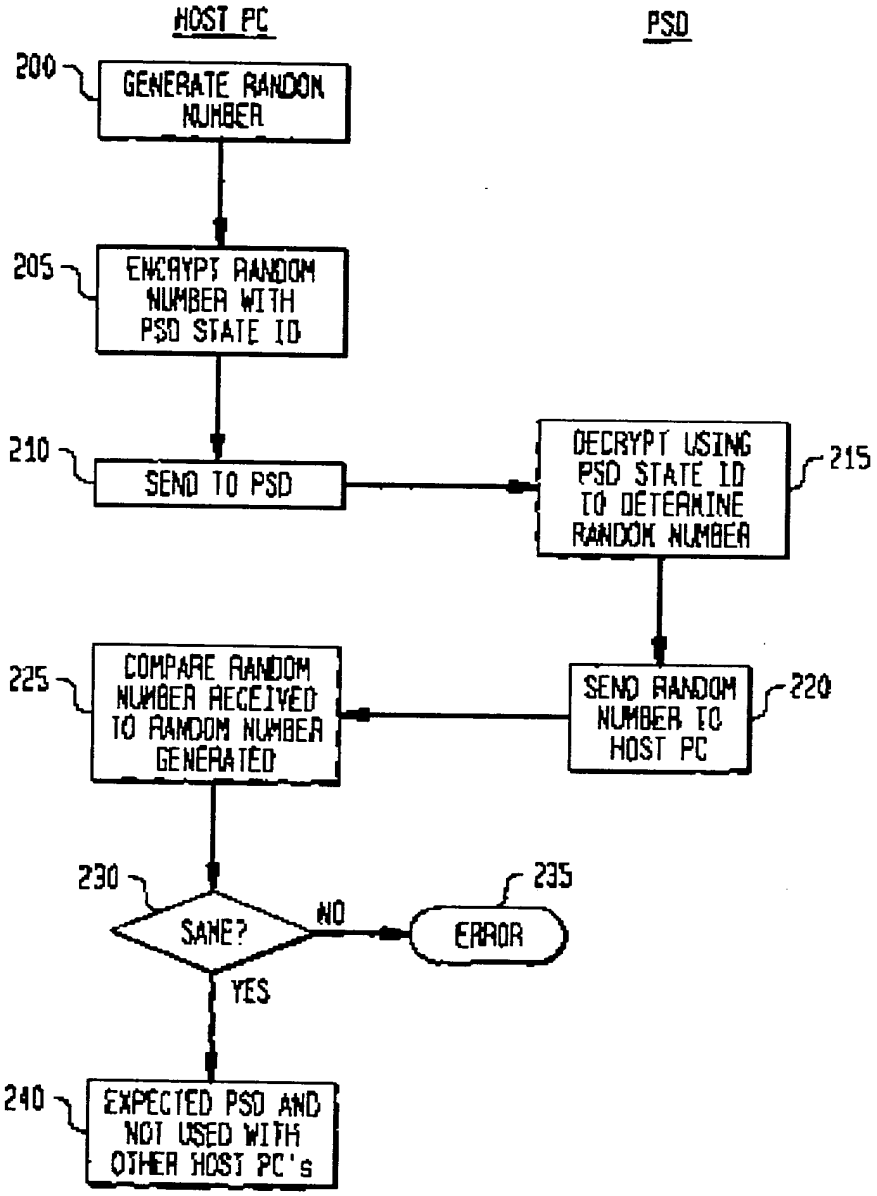


FIG. 2



PNSDOCID: <EP 0859340A2T1 >

FIG. 3



BNSDOCID: <EP___0859340A2T1_>

(19) Europäisches Patentamt
European Patent Office
Office uropé n d s brevets

(11) EP 0 859 340 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
13.09.2000 Bulletin 2000/37

(43) Date of publication A2:
19.08.1998 Bulletin 1998/34

(21) Application number: **97120460.7**

(22) Date of filing: **21.11.1997**

(51) Int. Cl.[7]: **G07B 17/00**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **21.11.1996 US 754578**

(71) Applicant: **PITNEY BOWES INC.**
Stamford, Connecticut 06926-0700 (US)

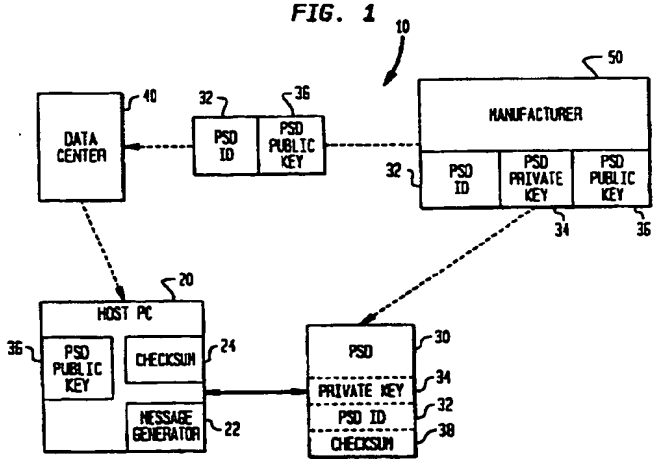
(72) Inventors:
- **Ryan, Frederick W., Jr.**
  Oxford, Connecticut 06478 (US)
- **Cordery, Robert A.**
  Danbury, Conn. 06811 (US)

(74) Representative:
Avery, Stephen John et al
Hoffmann Eitle,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Method for verifying the expected postage security device and its status

(57) A secure and reliable method for verifying in the host system that the expected PSD is coupled to the host system includes generating a random number in the host system and encrypting the random number with a PSD state identification number. The encrypted random number is then sent to the PSD. The PSD decrypts the encrypted random number received using the PSD state identification number and sends the decrypted random number to the host system. The host system compares the decrypted random number received from the PSD to the random number generated in the host system. If they are the same, the host system has verified the expected PSD and has also verified that the PSD has not completed any transactions apart from the host system. A method for verifying that the expected host is coupled to the PSD mirrors the method for verifying the expected PSD.

FIG. 1



EP 0 859 340 A3

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

BNSDOCID: <EP___0859340A3_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 12 0460

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	EP 0 388 843 A (ALCATEL SATMAM) 26 September 1990 (1990-09-26) * column 2, line 14 - line 41 * * column 9, line 40 - line 42 *	5,7,10	G07B17/00
A		1-4,6,8, 9,11-13	
Y	EP 0 298 776 A (ALCATEL BUSINESS SYSTEMS LIMITED) 11 January 1989 (1989-01-11) * column 5, line 23 - line 62 *	5,7,10	
A	"Information Based Indicia Program Host System Specification 'Draft!" 9 October 1996 (1996-10-09) , UNITED STATES POSTAL SERVICE XP002142880 * page 3-1, paragraph 3.1.2 *	1-13	
A	US 4 935 961 A (GARGIULO ET AL.) 19 June 1990 (1990-06-19) * column 1, line 60 - line 68 * * column 2, line 23 - line 32 * * column 2, line 50 - line 59 *	1-13	
A	GB 2 233 937 A (PITNEY BOWES PLC) 23 January 1991 (1991-01-23) * page 5, line 1 - page 6, line 16 *	1-13	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G07B G07F G06F
A	US 4 802 218 A (WRIGHT ET AL.) 31 January 1989 (1989-01-31) * column 9, line 44 - column 10, line 52 *	12	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	19 July 2000	Schofield, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP___0859340A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 97 12 0460

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-07-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 388843 A	26-09-1990	US 5107455 A	21-04-1992
		DE 69014362 D	12-01-1995
		DE 69014362 T	27-04-1995
		US 5612884 A	18-03-1997
		US 5369401 A	29-11-1994
EP 0298776 A	11-01-1989	GB 2208368 A	30-03-1989
		DE 3884485 D	04-11-1993
		DE 3884485 T	05-05-1994
		US 5323323 A	21-06-1994
US 4935961 A	19-06-1990	NONE	
GB 2233937 A	23-01-1991	US 5181245 A	19-01-1993
US 4802218 A	31-01-1989	AT 116778 T	15-01-1995
		AT 175512 T	15-01-1999
		AT 160456 T	15-12-1997
		AT 160039 T	15-11-1997
		AU 605443 B	10-01-1991
		AU 7961287 A	24-03-1988
		BR 8707450 A	06-12-1988
		CA 1320578 A	20-07-1993
		CA 1326911 A	08-02-1994
		CA 1335839 A	06-06-1995
		CA 1296809 A	03-03-1992
		DE 3750958 D	16-02-1995
		DE 3750958 T	08-06-1995
		DE 3752138 D	11-12-1997
		DE 3752138 T	26-03-1998
		DE 3752146 D	02-01-1998
		DE 3752146 T	09-04-1998
		DE 3752247 D	18-02-1999
		DE 3752247 T	10-06-1999
		DK 228888 A	17-06-1988
		EP 0294397 A	14-12-1988
		EP 0619563 A	12-10-1994
		EP 0619564 A	12-10-1994
		EP 0619565 A	12-10-1994
		EP 0740275 A	30-10-1996
		FI 882047 A,B,	02-05-1988
		JP 1500863 T	23-03-1989
		JP 2661932 B	08-10-1997
		NO 300660 B	30-06-1997
		WO 8801818 A	10-03-1988
		US 4864618 A	05-09-1989

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP___0859340A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 97 12 0460

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

19-07-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4802218 A		US 4900904 A	13-02-1990
		US 4900903 A	13-02-1990

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP___0859340A3_I_>